NIST issues identify management considerations for FirstNet

Fierce Mobile Government By Stephanie Kanowitz

April 22, 2015

As work moves forward on a nationwide public safety broadband network, the National Institute of Standards and Technology released guidelines for addressing identity management across the new system.

The First Responder Network Authority, or FirstNet, an independent agency under the Commerce Department, was established to develop, build and operate the first such network for use by first responders and other public safety employees during emergency situations. It would ultimately make communication among them more interoperable by basing the network on Long Term Evolution, a group of commercial standards, and commercial products. That means responders will be able to use cellular and high-bandwidth technologies in place of terrestrial radio, but it also means new security challenges.

NIST's report (pdf), released March 30, gives information on identity management and applicable federal and industry guidance for using next-generation networks, according to a release . The analysis covers topics such as selecting identity credentials, authentication processes and identity management technologies that could be used.

"This document repeatedly notes that selecting a single 'secure credential' is insufficient for securing a public safety organization's identity management infrastructure," the guidance states. "Individuals must undergo some degree of identify proofing before they are even given the opportunity to authenticate to a public safety system."

Overall, the recommendations won't fit every jurisdiction's needs, and in some areas, there are no panaceas, NIST said. For instance, the agency found no immediately implementable authentication approach that would work across the board. Additionally, rather than recommend specific technologies for various public safety workers, NIST looked at myriad options and left it to organizations to decide what's usable and secure.

Among the guidance NIST recommends are:

- The Office of Management and Budget's E-Authentication Guidance for Federal Agencies, which requires a five-step process including conducting a risk assessment of the government system based on four levels of assurance and periodically reassessing the system.
- Homeland Security Presidential Directive 12, which mandates a common identification standard and led to the creation of the Personal Identity Verification card.
- Its own Special Publication 800-63-2: Electronic Authentication Guideline, which defines technical requirements for identity spoofing, tokens and authentication protocols.

The guidance also addresses device and user identities in terms of bring-your-own-device scenarios in which responders might use personal devices to access the network. It also covers access via passwords or physical gestures, biometrics and remote authentication.

NIST's analysis is not the final word on securing the public safety network. The agency recommends future research as biometric capabilities for mobile devices emerge and as wearable technology gains traction, for instance.

Link to Article

Link to Fierce News Articles